

REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed October 25, 2007 (Paper No. 20071019). Upon entry of this response, claims 1-30 are pending in the application. No claims have been amended, cancelled or withdrawn in this response. Applicants respectfully request that there be reconsideration of all pending claims.

I. Allowable Subject Matter

Applicants appreciate the Examiner's allowance of claims 8-9 and 19-30. Applicants also acknowledge the Examiner's indication in the Office Action that claims 2-5, 7, 11-12, and 14-18 would be allowable if rewritten to include all of the limitations of the base claim and any intervening claims. However, Applicants choose not to rewrite allowable dependent claims 2-5, 7, 11-12, and 14-18 because Applicants believe that independent claims 1, 6, 10, and 13 are each allowable for at least the reasons presented below.

II. Rejection of Claims 1, 6, 10, and 13 under 35 U.S.C. §102

Claims 1, 6, 10, and 13 have been rejected under §102(e) as allegedly anticipated by *Candelore et al.* (U.S. 7,124,303). Applicants respectfully traverse this rejection. A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, e.g., *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

A. Independent Claim 1

1. *Candelore et al.* fails to teach, disclose or suggest at least "at least a portion of said unencrypted packets, at least one of said first encrypted packets, and at least one of said second encrypted packets are indistinguishable from one another based upon a packet identifier"

The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. The

cited portions of *Candelore et al.* does disclose “duplicating only certain packets tagged with a given PID” (Col. 5, lines 30-31), and further disclose “[t]he original (i.e. legacy) PID continues to tag the packets encrypted with legacy encryption as well as other packets sent in the clear. The new PID is used to tag packets encrypted by the second encryption method” (Col. 5, lines 33-36). However, the cited portions do not teach that at least one of the packets encrypted by the first scheme and at least one of the packets encrypted by the second scheme are indistinguishable from one another based on a packet identifier, as recited in claim 1. Instead, *Candelore et al.* teaches the opposite:

Packets with the secondary PID shadow the encrypted packets tagged with the primary PID. The packets making up the encrypted pairs can occur in either order but, in the preferred implementation, maintain sequence with the clear portion of the PID stream. By use of the primary and secondary PIDs, the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box.
(Col. 5, lines 36-47.)

Even if the terms “original PID” and “new PID” do not themselves imply that the original PID values is different, the teaching that the decoder uses the PIDs to determine which packets are to be decrypted implies that the original and new PIDs are **different**. In contrast, claim 1 requires that at least one of the packets encrypted by the first scheme and at least one of the packets encrypted by the second scheme are **indistinguishable from one another** based on a packet identifier. For at least the reason that *Candelore et al.* fails to disclose, teach or suggest this feature, Applicants respectfully submit that *Candelore et al.* does not anticipate claim 1. Therefore, Applicants request that the rejection of claim 1 be withdrawn.

2. *Candelore et al.* fails to teach, disclose or suggest at least “wherein said at least one each of said first and second encrypted packets...are also indistinguishable based upon a continuity count”

The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. Applicants have found no teaching in the cited portions of *Candelore et al.* that relates to a

continuity counter. A different portion of *Candelore et al.* does describe manipulation of continuity counters within encrypted content (Col. 22, line 54 to Col. 24, line 50). For example, *Candelore et al.* discloses that:

MPEG packets utilize a continuity counter to maintain the appropriate sequence of the packets. In order to assure proper decoding, this continuity counter should be properly maintained during creation of the packetized data stream at the headend. This is accomplished by assuring that packets with each PID are assigned continuity counters sequentially in a normal manner. Thus, packets with the secondary PID will carry a separate continuity counter from those of the primary PID.
(Col. 23, lines 1-10)

The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). For the encrypted packets, the primary PID and secondary PID are retained, but the continuity counters are swapped. Thus, the stream of packets can now be properly decrypted and decoded without errors caused by loss of continuity using the secondary PID.
(Col. 23, lines 45-55)

However, Applicants can find no relevant teaching in *Candelore et al.* that can properly correspond to a packet encrypted by a first scheme and a packet encrypted by a second scheme being indistinguishable from one another based on a continuity count. Therefore, the Office Action has not presented a proper *prima facie* case of anticipation by *Candelore et al.*, and the rejection of claim 1 should be withdrawn. Furthermore, if the rejection is maintained, the Examiner is requested to point out with particularity (in another non-final Office Action) which feature in *Candelore et al.* allegedly corresponds to the claimed feature discussed above.

B. Independent Claim 6

1. *Candelore et al.* fails to teach, disclose or suggest at least “reproducing a critical packet to produce duplicate packets having said identical packet identifier”

The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. The cited portions of *Candelore et al.* does disclose “duplicating only certain packets tagged with a

given PID” (Col. 5, lines 30-47). However, the cited portions do not teach “duplicate packets having said identical packet identifier” as recited in claim 6, but instead teach the opposite:

The original (i.e. legacy) PID continues to tag the packets encrypted with legacy encryption as well as other packets sent in the clear. The new PID is used to tag packets encrypted by the second encryption method. Packets with the secondary PID shadow the encrypted packets tagged with the primary PID. The packets making up the encrypted pairs can occur in either order but, in the preferred implementation, maintain sequence with the clear portion of the PID stream. By use of the primary and secondary PIDs, the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box.
(Col. 5, lines 33-47.)

Even if the terms “original PID” and “new PID” do not themselves imply that the original PID values is different, the teaching that the decoder uses the PIDs to determine which packets are to be decrypted implies that the original and new PIDs are different. In contrast, claim 6 recites that the duplicate packet has an “identical packet identifier”. For at least the reason that *Candelore et al.* fails to disclose, teach or suggest this feature, Applicants respectfully submit that *Candelore et al.* does not anticipate claim 6. Therefore, Applicants request that the rejection of claim 6 be withdrawn.

2. *Candelore et al.* fails to teach, disclose or suggest at least “distinguishing between said first and second encrypted packets...based upon the alignment of said first and second encrypted packets relative to one another”

The Office Action (p. 2) alleges that this *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. Applicants have reviewed *Candelore et al.* and have found no relevant teaching that can properly correspond to distinguishing between encrypted packets based upon the alignment of the packets relative to one another. Therefore, the Office Action has not presented a proper *prima facie* case of anticipation by *Candelore et al.*, and the rejection of claim 6 should be withdrawn. Furthermore, if the rejection is maintained, the Examiner is requested to point out with particularity (in another **non-final** Office Action) which feature in *Candelore et al.* allegedly corresponds to the claimed feature discussed above.

C. Independent Claim 8

1. *Candelore et al.* fails to teach, disclose or suggest at least “receiving second a second encrypted packet having said first packet identifier...wherein said first and second encrypted packets were encrypted according to first and second encryption schemes”

The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. The cited portions of *Candelore et al.* do disclose a system that “multiple encrypts only a portion of the data” (Abstract) and “duplicating only certain packets tagged with a given PID” (Col. 5, lines 30-47). However, the cited portions do not teach “a second encrypted packet having said first packet identifier” as recited in claim 8, but instead teach the opposite:

The original (i.e. legacy) PID continues to tag the packets encrypted with legacy encryption as well as other packets sent in the clear. The new PID is used to tag packets encrypted by the second encryption method. Packets with the secondary PID shadow the encrypted packets tagged with the primary PID. The packets making up the encrypted pairs can occur in either order but, in the preferred implementation, maintain sequence with the clear portion of the PID stream. By use of the primary and secondary PIDs, the decoder located in the set-top box can readily determine which packets are to be decrypted using the decryption method associated with that set-top box.
(Col. 5, lines 33-47.)

Even if the terms “original PID” and “new PID” do not themselves imply that the original PID values is different, the teaching that the decoder uses the PIDs to determine which packets are to be decrypted implies that the original and new PIDs are different. In contrast, claim 8 recites that the packet encrypted by the second encryption scheme has “said first packet identifier” of the packet encrypted by the first encryption scheme. For at least the reason that *Candelore et al.* fails to disclose, teach or suggest this feature, Applicants respectfully submit that *Candelore et al.* does not anticipate claim 8. Therefore, Applicants request that the rejection of claim 8 be withdrawn.

2. *Candelore et al.* fails to teach, disclose or suggest at least “distinguishing between said first and second encrypted packets based upon the order said first and second encrypted packets are received”

The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. Applicants have reviewed *Candelore et al.* and have found no relevant teaching that can properly correspond to distinguishing between encrypted packets based upon the order in which the packets are received. Therefore, the Office Action has not presented a proper *prima facie* case of anticipation by *Candelore et al.*, and the rejection of claim 8 should be withdrawn. Furthermore, if the rejection is maintained, the Examiner is requested to point out with particularity (in another **non-final** Office Action) which feature in *Candelore et al.* allegedly corresponds to the claimed feature discussed above.

D. Independent Claim 10

Applicants respectfully submit that independent claim 10 is allowable for at least the reason that *Candelore et al.* fails to teach, disclose or suggest at least “selecting one of said first and second encrypted content to decrypt based upon the alignment of said first and second encrypted content relative to one another”. The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. Applicants have reviewed *Candelore et al.* and have found no relevant teaching that can properly correspond to selecting content to decrypt based upon the relative alignment of the content. Therefore, the Office Action has not presented a proper *prima facie* case of anticipation by *Candelore et al.*, and the rejection of claim 10 should be withdrawn. Furthermore, if the rejection is maintained, the Examiner is requested to point out with particularity (in another **non-final** Office Action) which feature in *Candelore et al.* allegedly corresponds to the claimed feature discussed above.

E. Independent Claim 13

Applicants respectfully submit that independent claim 13 is allowable for at least the reason that *Candelore et al.* fails to teach, disclose or suggest at least “a decrypter that discards one of said first and second encrypted packets based upon the alignment of said first and second encrypted packets relative to one another and decrypts the other of said first and second encrypted packets”. The Office Action (p. 2) alleges that *Candelore et al.* discloses this feature in the Abstract, at Col. 5, lines 30-47, and Col. 6, lines 1-12. Applicants respectfully disagree. Applicants have reviewed *Candelore et al.* and have found no relevant teaching that can properly correspond to choosing to discard or to decrypt encrypted packets based on relative alignment of the packets relative to one another. Therefore, the Office Action has not presented a proper *prima facie* case of anticipation by *Candelore et al.*, and the rejection of claim 13 should be withdrawn. Furthermore, if the rejection is maintained, the Examiner is requested to point out with particularity (in another **non-final** Office Action) which feature in *Candelore et al.* allegedly corresponds to the claimed feature discussed above.

CONCLUSION

Applicants respectfully request that all outstanding objections and rejections be withdrawn and that this application and presently pending claims 1-30 be allowed to issue. Any statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and official notice, or statements interpreted similarly, should not be considered well known since the Office Action does not include specific factual findings predicated on sound technical and scientific reasoning to support such conclusions. If the Examiner has any questions or comments regarding Applicants' response, the Examiner is encouraged to telephone Applicants' undersigned counsel.

Respectfully submitted,

By: /Karen G. Hazzah/

Karen G. Hazzah, Reg. No. 48,472

**THOMAS, KAYDEN, HORSTEMEYER
& RISLEY, L.L.P.**

600 Galleria Parkway, NW
Suite 1500
Atlanta, Georgia 30339-5948
Tel: (770) 933-9500
Fax: (770) 951-0933